REMARKS

Claims 19-38 are pending in the present application. By this Response, claims 1-18 are canceled and claims 19-38 are added. Support for the subject matter recited in newly added claims 19-38 may be found at least in the originally filed claims 1-19, the specification at pages 9-12, and Figure 4. Reconsideration of the claims in view of the above amendments and the following remarks is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. Telephone Interview

Applicants thank Examiner Simitoski for the courtesies extended to Applicant's representative during the October 14, 2004 telephone interview. During the telephone interview Examiner Simitoski stated that the newly added claims appear to overcome the rejections under 35 U.S.C. § 112, first and second paragraphs. In addition, Applicant's representative discussed the distinctions of the present claims over the cited references. Examiner Simitoski stated that he understood Applicant's position with regard to the references and would take Applicant's arguments into consideration when examining the newly added claims. The substance of the telephone interview is summarized in the following remarks.

II. 35 U.S.C. § 112, First Paragraph

The Office Action rejects claims 1-18 under 35 U.S.C. § 112, first paragraph alleging that the claims contain subject matter which is not described in the specification in such a way as to enable one skill in the art to which it pertains to make and/or use the invention. Specifically, the Office Action alleges that it is unclear whether "authenticating the user password" involves the use of "the application's associated password." This rejection is moot in view of the cancellation of claims 1-18.

Newly added claims 22, 29 and 35 recite providing the application password and user password to a security service which performs authentication based on the application password and user password. This feature is described on page 11, lines 18-21 of the present specification. Authentication of passwords is generally known to those of ordinary skill in the art and one of ordinary skill in the art would be well aware of the processes involved in authenticating a password. Therefore, it is not necessary to set forth the specific details of authentication within the specification. The claims clearly state that the authentication is performed by a security services based on a supplied user password and application password. One of ordinary skill in the art would be able to provide a security service that authenticates a user password based on the user password and an application password using the present description and the knowledge of those of ordinary skill in the art. Thus, Applicant respectfully submits that the subject matter of claims 22, 29 and 35 is adequately described in the present specification to enable one skilled in the art to which it pertains to make and/or use the present invention.

III. 35 U.S.C. § 112, Second Paragraph

The Office Action rejects claims 1-18 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. This rejection is moot in view of the cancellation of claims 1-18. Claims 19-38 are added by this Response and all terms used in the claims have proper antecedent basis and all relationships of elements are clearly set forth in the claims.

IV. 35 U.S.C. § 103, Alleged Obviousness

The Office Action rejects claims 1-4, 6-10, 12-16 and 18 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Win et al. (U.S. Patent No. 6,182,142) in view of Compelson, "Password Officer 2000, The Complete Password Management Solution," Compelson Laboratories, and further in view of Edwards, "Understanding Network Security." This rejection is moot in view of the cancellation of claims 1-4, 6-10, 12-16 and 18. However, in order to expedite prosecution of this application, the following remarks regarding the references and distinctions set forth in the newly added claims 19-38 are provided for the Examiner's consideration.

Claim 19, which is representative of the other independent claims 26 and 33 with regard to similarly recited subject matter, reads as follows:

> 19. A method for retrieval of user passwords in a computer network, comprising:
>
> receiving, in a database server, a user identifier and user password from a client computing device via an application login;
>
> identifying an application associated with the application login; and
>
> identifying an application password, associated with the identified application and the user identifier, from a backend database associated with the database server, wherein the backend database stores entries for each of a plurality of registered users, and wherein the entries for the plurality of registered users include the user identifiers and application passwords for each application for which a user is registered, wherein at least one entry of the entries for each of the plurality of registered users has a plurality of different user identifiers and corresponding passwords, the plurality of different user identifiers and corresponding passwords comprising one user identifier and password for each application of a plurality of applications for which a user associated with the entry is registered. (emphasis added)

None of the cited prior art teaches or suggests the features of claim 19 emphasized above. Furthermore, as set forth hereafter, the alleged combination of references is improper and is not a valid basis upon which to reject claims 19-38.

Win is directed to a method and system for controlling access to information resources using a single sign-on that gives user access to authorized resources based on the user's role in the organization. Win specifically teaches that the user is granted access to a plurality of resources using a single sign-on, i.e. a single user ID and password. As stated on in column 9, lines 57-62:

> Preferably, a single login page is provided regardless of the number of Web applications to which the user has access. Thus, the system 2 provides single secure log-in to Intranet or Extranet Web applications. The login page provides a single universal point of access to authorized applications and content.

In fact, Win specifically teaches away from having multiple user IDs and passwords for a plurality of applications at column 6, lines 6-16 which reads as follows:

> The system 2 also enables Users to log-in to the system once, and thereafter access one or more Resources during an authenticated session. Users may log in either with a digital certificate or by opening a login page URL with a web browser and entering a name and password. In the past, users have had to log in individually to each Web application that they are authorized to user. In the preferred embodiment, users always access the same login page regardless of the number of resources to which they need access. Thus, the system provides a mechanism of single secure log-in to Web resources.

Thus, Win does not teach or suggest a backend database associated with a database server, wherein the backend database stores entries for each of a plurality of registered users, and wherein the entries for the plurality of registered users include the user identifiers and application passwords for each application for which the user is registered, and wherein at least one entry of the entries for each of the plurality of registered users has a plurality of different user identifiers and corresponding passwords, the plurality of different user identifiers and corresponding passwords comprising one user identifier and password for each application of a plurality of applications for which a user associated with the entry is registered. To the contrary, Win teaches the use of a single user ID and password for a plurality of resources and specifically teaches away from having multiple user IDs and passwords, one for each application that a user is registered to use.

Compelson teaches a software product entitled the Password Officer 2000 which is a client or stand-alone computer based software product for managing passwords. The Password Officer 2000 permits a user to set up a list of applications and their corresponding user IDs and passwords. When a user ID and password is required, the Password Office 2000 will enter the user ID and password. The Password Officer 2000 will automatically enter whole sequences upon recognition of a specific application that requires it or the user can select which one to enter and where.

The Password Officer 2000 is a client or stand-alone computer based mechanism. That is, the list of applications, user IDs and passwords must be maintained at the user's client machine. Thus, Compelson does not teach or suggest receiving, in a database server, a user identifier and user password from a client computing device via an application login. Furthermore, Compelson does not teach or suggest identifying an application password from a backend database associated with the database server, wherein the backend database stores entries for each of a plurality of registered users, as recited in claim 19. To the contrary, the Password Officer 2000 product described in Compelson is concerned with storing the passwords and user IDs for a single user in a client computing device and is not concerned with storing user IDs and passwords for a plurality of applications for each of a plurality of users in a backend database associated with a database server.

Edwards is cited as allegedly teaching that good password policy is to never use the same password for multiple systems. While this may be a good password policy, this does not teach the features of receiving, in a database server, a user identifier and user password from a client computing device via an application login, identifying an application password from a backend database associated with the database server, the backend database storing entries for each of a plurality of registered users, the entries for the plurality of registered users including the user identifiers and application passwords for each application for which a user is registered, or at least one entry of the entries for each of the plurality of registered users has a plurality of different user identifiers and corresponding passwords, the plurality of different user identifiers and corresponding passwords comprising one user identifier and password for each application of a plurality of applications for which a user associated with the entry is registered, as recited in claim 19.

Thus, none of the cited references teach or suggest the features of claim 19. Furthermore, one of ordinary skill in the art would not have found it obvious to combine the references in the manner alleged by the Office Action. This is because the primary reference specifically teaches away from the alleged combination. Win specifically teaches that a single-login mechanism is desired and that having multiple user IDs and passwords for a plurality of resources is undesirable. Compelson teaches the opposite and provides a mechanism for storing multiple user IDs and passwords for a plurality of different applications. Thus, one of ordinary skill in the art would not have found it obvious to combine two references that teach away from each other. The only reason one of ordinary skill in the art would even attempt such a combination would be if that person were attempting to recreate the claimed invention having first had benefit of Applicant's disclosure. This is impermissible hindsight reconstruction using Applicant's own disclosure as a guide and is not a valid basis upon which to make a rejection under 35 U.S.C. § 103(a).

Furthermore, it is not at all clear how the mechanisms of Compelson and Win would be combined even if one were to ignore the specific teachings away from the combination. Win specifically teaches a single login mechanism while Compelson teaches having multiple user IDs and passwords for a plurality of applications. Because these teachings are diametrically opposed to one another, it is not clear how one could integrate them into a single mechanism as alleged by the Office Action without destroying the intended operation of each mechanism.

The Edwards reference is only combined with Win and Compelson as teaching a desirable password policy of having different passwords for multiple systems. Again, this seems to teach away from the specific teachings of Win. Thus, Edwards actually teaches against the alleged combination of Win and Compelson.

Therefore, in view of the above, Applicant respectfully submits that neither Win, Compleson, nor Edwards, whether taken alone or in combination, teach or suggest the features of independent claim 19 or similar features found in independent claims 26 and 33. At least by virtue of their dependency on claims 19, 26 and 33, neither Win, Compelson nor Edwards, whether taken alone or in combination, teach or suggest the features of dependent claims 20-25, 27-32 and 34-38.

In addition to the above, none of the cited references, either alone or in combination, teach or suggest the referral object recited in claims 20, 25, 27, 32, 34 and 38. The Office Action rejected this feature, as originally presented in claim 4, based on a combination of Win, Compelson, Edwards and Prompt (U.S. Patent Application Publication 2001/0034733). The Office Action alleged that Prompt taught this feature in paragraph 120 which reads as follows:

> The VDS provides unlimited LDAP extensibility to any existing LDAP directory implementation using the object referral mechanism. Object referral allows one LDAP directory to make reference to another LDAP directory when clients request objects or attributes that are not stored in the primary directory. Using object referral, the VDS enables the extension of an existing LDAP structure without the necessity for directory redesign. With the present invention, objects and attributes can be added to an existing directory structure quickly to accommodate the changing needs of the client applications.

While this section of Prompt describes the object referral mechanism of an LDAP directory, Prompt provides no teaching or suggestion to use a referral object to identify an application password, wherein the referral object references a storage location in a backend database where user identifiers and application passwords associated with a user identifier are stored. To the contrary, Prompt merely provides the general teaching of using object referral to add objects and attributes to an existing directory structure to "quickly accommodate the changing needs of the client applications." Prompt makes no mention or even suggestion regarding using referral objects to access user identifiers and passwords for a received user identifier. Thus, even if Prompt were combinable with Win, Compelson and Edwards, despite the fundamental problems with this combination discussed above, the result would still not be the invention as recited in claims 20, 25, 27, 32, 34 and 38.

V. Conclusion

It is respectfully urged that the subject application is patentable over Win, Compelson, Edwards and Prompt and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: October 14, 2004

Stephen J. Walder, Jr.
Reg. No. 41,534
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorney for Applicant